PCT/JP2004/000619

23.1.2004

#2

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月２３日

出願番号
Application Number: 特願２００３－０１５２３３

[ST. 10/C]: [Ｊ.Ｐ２００３－０１５２３３]

出願人
Applicant(s): キヤノン株式会社

２００４年　２月２６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０１３６４７

【書類名】　特許願
【整理番号】　251739
【提出日】　平成15年 1月23日
【あて先】　特許庁長官殿
【国際特許分類】　G06F　7/00
【発明の名称】　情報処理方法
【請求項の数】　1
【発明者】
　【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
　【氏名】　林　淳一
【発明者】
　【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
　【氏名】　須賀　祐治
【特許出願人】
　【識別番号】　000001007
　【氏名又は名称】　キヤノン株式会社
【代理人】
　【識別番号】　100076428
　【弁理士】
　【氏名又は名称】　大塚　康徳
【選任した代理人】
　【識別番号】　100112508
　【弁理士】
　【氏名又は名称】　高柳　司郎

【選任した代理人】
　【識別番号】　100115071
　【弁理士】
　【氏名又は名称】　大塚　康弘
【選任した代理人】
　【識別番号】　100116894
　【弁理士】
　【氏名又は名称】　木村　秀二
【手数料の表示】
　【予納台帳番号】　003458
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0102485
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理方法

【特許請求の範囲】

【請求項１】　符号化画像データを暗号化する情報処理方法であって、

符号化画像データを入力する工程と、

入力した符号化画像データを暗号化する工程と、

符号化データのヘッダ部中の誤り検出符号有無を示す有無情報を、誤り検出符号無しに変更し、暗号化した符号化画像データを出力する工程と

を備えることを特徴とする情報処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル画像データの圧縮符号化したデータを暗号化する技術に関するものである。

【０００２】

【従来の技術】

従来、画像データなどを秘匿して伝送するために、画像データ全体の暗号化やスクランブルなどが行なわれてきた。これは、予め画像データ全体、或いはその一部を暗号鍵を用いて暗号化し、前記暗号鍵に対応する復号鍵を有するものだけが正しく復号することが可能であるようにする技術である。

【０００３】

一方、画像データは情報量が大きい為に、これを効率的に伝送、及び蓄積する際に圧縮符号化を行う場合が多い。圧縮符号化としては、例えばＩＳＯ／ＩＥＣＪＴＣ　１／ＳＣ　２９／ＷＧ１にて標準化されているＪＰＥＧ２０００と呼ばれる技術などが有望視されている。従って、前述した画像データの暗号化はＪＰＥＧ２０００のような圧縮符号化された画像データに対して施されることが望まれる。

【０００４】

ＪＰＥＧ２０００においては、たとえ伝送過程で誤りが生じた場合でも、その

誤りを検知する機能を適応することが可能である。送信側で、この機能を用いて画像データを圧縮符号化して送信することによって、受信側で圧縮復号の際に誤りを検知した場合でも、誤っている部分のデータだけを再送するように送信側に再送要求を出し、再送されたデータを圧縮復号することによって、正しく復号可能となる。

【０００５】

【発明が解決しようとする課題】

しかしながら、前述したように、誤り検出可能なように画像データを圧縮符号化し、更に、この圧縮符号化された画像データに対して暗号化処理を施した場合、誤り検知機能が正しく動作しない場合がある。これは、受信側において、暗号化された画像データを、（誤って）誤りが生じた画像データであると判定するからである。この場合、誤っていると判定された部分の再送要求を送信側にしたとしても、送信側から送られてくるのは当然のことながら（誤っていると判断された部分と）同じ画像データであり、場合によっては繰り返し再送要求をし続けることにもなりかねない。

【０００６】

本発明はかかる問題点に鑑みなされたものであり、誤り検出符号が付加された圧縮符号化画像データを暗号化したとしても、それを受信し再生する側の装置において無意味な再送要求等を行わず、正常な処理を行えるようにする技術を提供しようとするものである。

【０００７】

【課題を解決するための手段】

この課題を解決するため、例えば本発明の情報処理方法は以下のような工程を備える。すなわち、

符号化画像データを暗号化する情報処理方法であって、

符号化画像データを入力する工程と、

入力した符号化画像データを暗号化する工程と、

符号化データのヘッダ部中の誤り検出符号有無を示す有無情報を、誤り検出符号無しに変更し、暗号化した符号化画像データを出力する工程とを備える。

【０００８】

【発明の実施の形態】

以下、添付図面に従って本発明に係る実施形態を説明する。

【０００９】

＜全体構成の説明＞

実施形態におけるシステム概要例を図９に示す。図中、９０はインターネットであって、９１は例えばデジタルカメラやイメージスキャナ、フィルムスキャナ等で撮像した画像データを圧縮符号化＆暗号化処理を行う装置である。９２は画像データを受信し、復号する装置、９３は復号する際に必要となる暗号化解除鍵を記憶している認証サーバある。装置９１乃至９３はパーソナルコンピュータ等の汎用装置で構わない。処理の流れを簡単に説明すると、次の通りである。

【００１０】

装置９１では、所望とする画像データを圧縮符号化及び暗号化処理を行い、インターネット９０を介して配布する。配布するのは装置９１が直接行ってもよいし、適当なサーバを介して配布しても構わない。ただし、暗号化されている関係で、その解除するために必要な鍵情報を、その画像データを特定する情報（例えばＩＤ）と共に認証サーバ９３が有するＤＢに登録しておく。画像復号装置９２は所望とする画像を受信し、復号を行ない閲覧するものであるが、暗号化されている画像データを閲覧するには、認証サーバ９３にその画像を特定する情報を通知して、暗号化解除鍵情報を要求する。この結果、暗号化解除鍵情報が認証サーバ９３より受信するので、それを用いて暗号化を解除し、復号再生する。

【００１１】

＜圧縮符号化処理部＞

まずはじめに、図１を用いて、画像データ圧縮＆暗号化装置９１における圧縮符号化処理、及びその過程で実行される誤り検出符号化機能を説明する。

【００１２】

図１において、１１は画像入力部、１２は離散ウェーブレット変換部、１３は量子化部、１４はエントロピ符号化部、１５は符号出力部である。まず、画像入力部１１に対して符号化対象となる画像を構成する画素信号がラスタースキャン

順に入力され、その出力は離散ウェーブレット変換部１２に入力される。以降の説明では画像信号はモノクロの多値画像を表現しているが、カラー画像等、複数の色成分を符号化するならば、ＲＧＢ各色成分、或いは輝度、色度成分を上記単色成分として圧縮すればよい。

【００１３】

離散ウェーブレット変換部１２は、入力した画像信号に対して２次元の離散ウェーブレット変換処理を行い、変換係数を計算して出力するものである。図２（ａ）は離散ウェーブレット変換部１２の基本構成を表したものであり、入力された画像信号はメモリ２１に記憶され、処理部２２により順次読み出されて変換処理が行われ、再びメモリ２１に書きこまれており、本実施の形態においては、処理部２２における処理の構成は同図（ｂ）に示すものとする。同図において、入力された画像信号は遅延素子およびダウンサンプラの組み合わせにより、偶数アドレスおよび奇数アドレスの信号に分離される。すなわち、入力される画素データは、ここで偶数番めの画素と奇数番目の画素に分けられることになる。分離された夫々の画素データは、２つのフィルタｐおよびｕによりフィルタ処理が施される。同図ｓおよびｄは、各々１次元の画像信号に対して１レベルの分解を行った際のローパス係数およびハイパス係数を表しており、次式により計算されるものとする。

$$d(n) = x(2*n+1) - \mathrm{floor}((x(2*n) + x(2*n+2))/2) \qquad (式１)$$

$$s(n) = x(2*n) + \mathrm{floor}((d(n-1) + d(n))/4) \qquad (式２)$$

ただし、x(n)は変換対象となる画像信号である。

【００１４】

以上の処理により、画像信号に対する１次元の離散ウェーブレット変換処理が行われる。２次元の離散ウェーブレット変換は、１次元の変換を画像の水平・垂直方向に対して順次行うものであり、その詳細は公知であるのでここでは説明を省略する。図２（ｃ）は２次元の変換処理により得られる２レベル（ウエーブレット変換回数が「２」という意味）の変換係数群の構成例であり、画像信号は異なる周波数帯域の係数列ＨＨ１、ＨＬ１、ＬＨ１、…、ＬＬに分解される。なお、以降の説明ではこれらの係数列をサブバンドと呼ぶ。各サブバンドの係数は後

続の量子化部１３に出力される。

【００１５】

量子化部１３は、入力した係数を所定の量子化ステップにより量子化し、その量子化値に対するインデックスを出力する。ここで、量子化は次式により行われる。

$q = sign(c)\ floor(abs(c) / \Delta)$　　（式３）

$sign(c) = 1;\ c \geqq 0$　　（式４）

$sign(c) = -1;\ c < 0$　　（式５）

ここで、ｃは量子化対象となる係数である。また、本実施の形態においてはΔの値として１を含むものとする。この場合実際に量子化は行われず、量子化部１３に入力された変換係数はそのまま後続のエントロピ符号化部１４に出力される。

【００１６】

エントロピ符号化部１４は入力した量子化インデックスをビットプレーンに分解し、ビットプレーンを単位に２値算術符号化を行ってコードストリームを出力する。図３はエントロピ符号化部１４の動作を説明する図であり、この例においては４×４の大きさを持つサブバンド内の領域において非０の量子化インデックスが３個存在しており、それぞれ＋１３、－６、＋３の値を持っている。エントロピ符号化部１４はこの領域を走査して最大値Ｍを求め、次式により最大の量子化インデックスを表現するために必要なビット数Ｓを計算する。

$S = ceil(log2(abs(M)))$　　（式８）

ここでｃｅｉｌ（ｘ）はｘ以上の整数の中で最も小さい整数値を表す。

【００１７】

図３においては、最大の係数値は１３であるのでＳは４であり、シーケンス中の１６個の量子化インデックスは同図（ｂ）に示すように４つのビットプレーンを単位として処理が行われる。最初にエントロピ符号化部１４は最上位ビットプレーン(同図ＭＳＢで表す)の各ビットをエントロピ符号化（本実施の形態では２値算術符号化）し、ビットストリームとして出力する。次にビットプレーンを１レベル下げ、以下同様に対象ビットプレーンが最下位ビットプレーン（同図ＬＳ

Ｂで表す）に至るまで、ビットプレーン内の各ビットを符号化し符号出力部１５に出力する。なお上記エントロピ符号化時において、各量子化インデックスの符号は、上位から下位へのビットプレーン走査において最初（最上位）に符号化されるべき非０ビットが検出されるとそのすぐ後に当該量子化インデックスの正負符号を示す１ビットを続けて２値算術符号化することとする。これにより、０以外の量子化インデックスの正負符号は効率良く符号化される。

【００１８】

ここで、本実施形態における誤り検出符号化について図１０を用いて説明する。図１０において、１０１は前述した一つのビットプレーン内の各ビットの並びである。また、１０２は誤り検出符号化のために１０１の後に添付される所定の情報である。以降では、この所定の情報をセグメンテーションシンボルと呼ぶ。本実施形態における誤り検出符号化は、図１０に示すように、本来エントロピ符号化される情報（１０１）の後にセグメンテーションシンボル（１０２）を添付した情報全体をエントロピ符号化するようにして実行する。尚、前記セグメンテーションシンボルは、圧縮符号化処理部と後述する圧縮復号処理部において同じ値を用いるようにする。

【００１９】

図４は、このようにして生成され出力される符号列の構成を表した概略図である。同図（ａ）は符号列の全体の構成を示したものであり、ＭＨはメインヘッダ、ＴＨはタイルヘッダ、ＢＳはビットストリームである。メインヘッダＭＨは同図（ｂ）に示すように、符号化対象となる画像のサイズ（水平および垂直方向の画素数）、画像を複数の矩形領域であるタイルに分割した際のサイズ、各色成分数を表すコンポーネント数、各成分の大きさ、ビット精度を表すコンポーネント情報から構成されている。なお、本実施の形態では画像はタイルに分割されていないので、タイルサイズと画像サイズは同じ値を取り、対象画像がモノクロの多値画像の場合コンポーネント数は１である。

【００２０】

次にタイルヘッダＴＨの構成を図４（ｃ）に示す。タイルヘッダＴＨには当該タイルのビットストリーム長とヘッダ長を含めたタイル長および当該タイルに対

する符号化パラメータから構成される。符号化パラメータには離散ウェーブレット変換のレベル、フィルタの種別等が含まれている。更に、前述した誤り検出符号化が適用されているか否かを示す情報も、この符号化パラメータに含まれている。以降では、この誤り検出符号が適用されているか否かを示す情報（１ビットで良い）を「第１の誤り検出符号化情報」と呼ぶ。そして、第１の誤り検出符号化情報が“０”の時には誤り検出符号化はされていないことを示し、一方で第１の誤り検出符号化情報が“１”の場合には誤り検出符号化されていることを示すことにする。

【００２１】

本実施の形態におけるビットストリームの構成を同図（ｄ）に示す。同図において、ビットストリームは各サブバンド毎にまとめられ、解像度の小さいサブバンドを先頭として順次解像度が高くなる順番に配置されている。さらに、各サブバンド内は上位ビットプレーンから下位ビットプレーンに向かい、ビットプレーンを単位として符号が配列されている。

【００２２】

上記符号配列とすることにより、後述する図８の様な階層的復号化を行うことが可能となる。

【００２３】

上述した実施の形態において、符号化対象となる画像全体の圧縮率は量子化ステップΔを変更することにより制御することが可能である。

【００２４】

また別の方法として本実施の形態では、エントロピ符号化部１４において符号化するビットプレーンの下位ビットを必要な圧縮率に応じて制限（廃棄）することも可能である。この場合には、全てのビットプレーンは符号化されず上位ビットプレーンから所望の圧縮率に応じた数のビットプレーンまでが符号化され、最終的な符号列に含まれる。

【００２５】

＜圧縮復号処理部＞

次に以上述べた圧縮符号化処理部による符号列を復号する方法、及び誤り検出

機能について説明する。図５は本実施の形態における圧縮復号化処理部の構成を表すブロック図であり、５１が符号入力部、５２はエントロピ復号部、５３は逆量子化部、５４は逆離散ウェーブレット変換部、５５は画像出力部である。

【００２６】

符号入力部５１は符号列を入力し、それに含まれるヘッダを解析して後続の処理に必要なパラメータを抽出し必要な場合は処理の流れを制御し、あるいは後続の処理ユニットに対して該当するパラメータを送出するものである。また、符号列に含まれるビットストリームはエントロピ復号部５２に出力される。

【００２７】

エントロピ復号部５２はビットストリームをビットプレーン単位で復号し、出力する。この時の復号化手順を図６に示す。図６（ａ）は復号対象となるサブバンドの一領域をビットプレーン単位で順次復号化（４プレーン時の場合）し、最終的に量子化インデックスを復元する流れを図示したものであり、同図の矢印の順にビットプレーンが復号される。復元された量子化インデックスは逆量子化部５３に出力される。

【００２８】

ここで、本実施形態における誤り検出機能について説明する。誤り検出符号化されているか否かは、入力された符号列中に含まれるヘッダを解析し、ヘッダ中の符号化パラメータに含まれる第１の誤り検出符号化情報により判定可能である。第１の誤り検出符号化情報が“１”の場合（誤り検出符号化されていると判定された場合）には、エントロピ復号された後のビットプレーンのうち、添付されたセグメンテーションシンボル（図１０における１０２）が、前述した符号化処理部において添付したセグメンテーションシンボルと一致するか否かを調べる。一致する場合には、誤りは生じていないと判定でき、一致しない場合には誤りが生じていると判定できる。誤りが生じている場合には、該ビットプレーンを送信側に再送するようにすれば正しく圧縮復号可能となる。

【００２９】

次に、逆量子化部５３は入力した量子化インデックスから、次式に基づいて離散ウェーブレット変換係数を復元する。

c' = Δ * q; q ≠ 0　　（式９）

c' = 0　　; q = 0　　（式１０）

ここで、qは量子化インデックス、Δは量子化ステップであり、Δは符号化時に用いられたものと同じ値である。c'は復元された変換係数であり、符号化時ではsまたはdで表される係数の復元したものである。変換係数c'は後続の逆離散ウェーブレット変換部５４に出力される。

【００３０】

図７は逆離散ウェーブレット変換部５４の構成および処理のブロック図を示したものである。同図（ａ）において、入力された変換係数はメモリ７１に記憶される。処理部７２は１次元の逆離散ウェーブレット変換を行い、メモリ７１から順次変換係数を読み出して処理を行うことで、２次元の逆離散ウェーブレット変換を実行する。２次元の逆離散ウェーブレット変換は、順変換と逆の手順により実行されるが、詳細は公知であるので説明を省略する。また同図（ｂ）は処理部７２処理ブロックを示したものであり、入力された変換係数はｕおよびｐの２つのフィルタ処理を施され、アップサンプリングされた後に重ね合わされて画像信号ｘ'が出力される。これらの処理は次式により行われる。

x'(2*n) = s'(n) - floor ((d'(n-1) + d'(n))/4)　　（式１５）

x'(2*n+1) = d'(n) + floor ((x'(2*n) + x'(2*n+2))/2)　　（式１６）

ここで、（式１）、（式２）、および（式１５）、（式１６）による順方向および逆方向の離散ウェーブレット変換は完全再構成条件を満たしているため、本実施形態において量子化ステップΔが１であり、ビットプレーン復号において全てのビットプレーンが復号されていれば、復元された画像信号ｘ'は原画像の信号ｘと一致する。

【００３１】

以上の処理により画像が復元されて画像出力部５５に出力される。 画像出力部５５はモニタ等の画像表示装置であってもよいし、あるいは磁気ディスク等の記憶装置であってもよい。

【００３２】

以上述べた手順により画像を復元表示した際の、画像の表示形態について図８

を用いて説明する。同図（ａ）は符号列の例を示したものであり、基本的な構成は図４に基づいているが、画像全体をタイルと設定されており、従って符号列中には唯一のタイルヘッダおよびビットストリームが含まれている。ビットストリームＢＳ０には図に示すように、最も低い解像度に対応するサブバンドであるＬＬから順次解像度が高くなる順に符号が配置されている。

【００３３】

圧縮復号処理部はこのビットストリームを順次読み込み、各サブバンドに対応する符号を復号した時点で画像を表示する。同図（ｂ）は各サブバンドと表示される画像の大きさの対応を示したものである。この例では２次元の離散ウェーブレット変換が２レベルであり、ＬＬのみを復号・表示した場合は原画像に対して画素数が水平および垂直方向に１／４縮小された画像が復元される。更にビットストリームを読み込み、レベル２のサブバンド全てを復号して表示した場合は、画素数が各方向に１／２に縮小された画像が復元され、レベル１のサブバンド全てが復号されれば、原画像と同じ画素数の画像が復元される。

【００３４】

上述した実施の形態において、エントロピ復号部５２において復号する下位ビットプレーンを制限（無視）することで受信或いは処理する符号化データ量を減少させ、結果的に圧縮率を制御することが可能である。この様にすることにより、必要なデータ量の符号化データのみから所望の画質の復号画像を得ることが可能である。また、符号化時の量子化ステップΔが１であり、復号時に全てのビットプレーンが復号された場合は、復元された画像が原画像と一致する可逆符号化・復号化を実現することもできる。

【００３５】

＜暗号符号化処理部＞

次に、図１１を用いて本実施の形態に適応可能な暗号符号化処理部について説明する。

【００３６】

図１１において、１１１は符号入力部、１１２は暗号化処理部、１１３は符号出力部である。図示において、符号入力部１１１は、図１における符号出力部１

５の出力結果を入力するものと考えれば分かりやすい。

【００３７】

符号入力部１１１は符号列を入力し、それに含まれるヘッダを解析して後続の処理に必要なパラメータを抽出し、後続の処理ユニットに対して該当するパラメータを送出するものである。また符号列に含まれるビットストリームは暗号化処理部１１２に出力される。

【００３８】

暗号化処理部１１２には、前記ビットストリームが入力され、操作者の指定や予め設定された情報（例えばハードディスクに記憶しておく）に従って、前記ビットストリームが暗号化処理され、暗号化されたビットストリームが出力される。

【００３９】

ここで、暗号化処理部１１２で実行される暗号化処理について、図１２を用いて説明する。図１２は、本実施形態に適応可能な暗号化処理を示すフローチャートである。

【００４０】

まず、ステップＳ１２１において、入力されたビットストリームが誤り検出符号化されているか否かが判定される。これは、前段の符号入力部１１１において解析された符号化パラメータに含まれる第１の誤り検出符号化情報を用いて判定可能である。第１の誤り検出符号化情報が“１”の場合（誤り検出符号化されていると判定された場合）には処理をステップＳ１２２に進め、第１の誤り検出符号化情報が“０”の場合（誤り検出符号化されていないと判定された場合）には処理をステップＳ１２４に進める。

【００４１】

ステップＳ１２２では、前記第１の誤り検出符号化情報を“０”に変更する。即ち、あたかも「誤り検出符号化されていない」ような情報に変更する。これは、後述するステップＳ１２４における暗号化処理によって、圧縮復号処理部での誤り検出検出機能が、「誤りが生じている」と誤判定するのを防止するためである。第１の誤り検出符号化情報を“０”とすることにより、圧縮復号処理部で誤

り検出検出機能は動作しないが、「誤りが生じている」と誤判定することは防止できる。ステップＳ１２２の後、処理をステップＳ１２３に進める。

【００４２】

ステップＳ１２３では、前記第１の誤り検出符号化情報とは異なる第２の誤り検出符号化情報を“１”に設定する。第２の誤り検出符号化情報は、「暗号化される前のビットストリームが誤り検出符号化されているか否かを示す」情報である。第２の誤り検出符号化情報が“１”の場合には、暗号化される前のビットストリームが誤り検出符号化されていたことを示し、一方で、第２の誤り検出符号化情報が“０”の場合には、暗号化される前のビットストリームが誤り検出符号化されていなかったことを示す。第２の誤り検出符号化情報は、前述したステップＳ１２２において誤り検出符号化情報を変更したことを補うために、後述する暗号復号処理部において用いられる。つまり、元々存在していた誤り検出符号化情報を待避することと等価の処理を行う。

【００４３】

また、第２の誤り検出符号化情報はヘッダ部分や、或いは、ヘッダ部分に含まれるコメントとして記録したりすればよい。或いは、第２の誤り検出符号化情報をビットストリームの所定の位置に添付し、後段の暗号化処理においてビットストリームと共に暗号化し、暗号文の中に含まれるようにしても構わない。

【００４４】

さて、ステップＳ１２４では、入力されたビットストリームに暗号化処理が施される。暗号化処理としては、入力されたビットストリームに含まれるデータの全てを暗号化するようにしてもよいし、一部分だけを部分的に暗号化するようにしてもよい。部分的に暗号化することにより、暗号化されていない部分は誰でも閲覧可能であるが、暗号化された部分は許可されたユーザだけが閲覧可能となるようなアクセス制御が可能である。

【００４５】

本発明においては暗号化対象は特に限定されることなく、前述した所定のサブバンドやビットプレーンやタイルなどの種々のデータを暗号化対象とすることが可能であることは明らかである。また、本発明においては暗号化処理は特に限定

されることなく、ＤＥＳ、ＡＥＳ、ＲＳＡなどの種々の暗号化方式が適応可能であることは明らかである。

【００４６】

尚、本実施形態においてはステップＳ１２１、ステップＳ１２２、及びステップＳ１２３の後にステップＳ１２４を処理するようにしたが、ステップＳ１２４の後に、ステップＳ１２１、ステップＳ１２２、及びステップＳ１２３を処理するようにしてもよい。

【００４７】

以上説明したような処理により生成されたヘッダ情報や暗号化されたビットストリームは後段の符号出力部１１３に出力される。

【００４８】

符号出力部１１３には、前段の暗号化処理部１１２で生成されたヘッダ情報や暗号化されたビットストリームが入力され、暗号化された符号列として出力される。

【００４９】

以上説明したように本実施形態によれば、画像符号化データを入力し、暗号化を行った場合、例え誤り訂正符号が付加されたとしても、誤り訂正符号無しにすることで、復号する側（例えばＰＣ）が画像データに誤りがあると誤認識することを避けることができるようになる。

【００５０】

なお、上記暗号化する側で行った暗号化済みの符号化データを受信した、復号化する側の装置では、暗号化を解除しない限りは正常な画像データにまで復号できない。換言すれば、復号化する側の装置では、何らかの手段を用いて、暗号化解除鍵情報を取得する必要になる。簡単には、復号化する側が暗号化する側に対して解除鍵を要求することであろうが、例えば双方がインターネット等のネットワークに接続する形態を採っている場合には、画像データを特定する情報と解除鍵情報を管理する認証サーバを設置し、その画像を特定する情報を受信した場合にその解除鍵情報を要求元に送信する形態を採用すれば良いであろう。

【００５１】

以上、本実施形態における暗号符号化処理部における動作について説明した。上記本実施形態における暗号符号化処理部は、一般に、パーソナルコンピュータ等の情報処理装置で実現できることは容易に類推できよう。また、パーソナルコンピュータ等の情報処理装置で、上記機能を実現すれば良いわけであるから、実施形態での特徴は情報処理方法、更には、コンピュータプログラムや、コンピュータプログラムを格納するＣＤＲＯＭ等のコンピュータ可読記憶媒体にまで及ぶものである。

【００５２】

＜暗号復号処理部＞

次に、図１３を用いて本実施の形態に適応可能な暗号復号処理部について説明する。

【００５３】

図１３において、１３１は符号入力部、１３２は暗号復号処理部、１３３は符号出力部である。図５に示す復号装置における符号入力部５１は、符号出力部１３３から出力された符号データを入力すると考えると分かりやすい。

【００５４】

符号入力部１３１は符号列を入力し、それに含まれるヘッダを解析して後続の処理に必要なパラメータを抽出し、後続の処理ユニットに対して該当するパラメータを送出するものである。また符号列に含まれるビットストリームは暗号復号処理部１３２に出力される。

【００５５】

暗号復号処理部１３２には、前記ビットストリームが入力され、前記ビットストリームが暗号復号処理され、暗号復号処理されたビットストリームが出力される。

【００５６】

ここで、暗号復号処理部１３２で実行される暗号化処理について、図１４を用いて説明する。図１４は、本実施形態に適応可能な暗号復号処理を示すフローチャートである。

【００５７】

まず、ステップＳ１４１において入力されたビットストリームが、暗号化前に誤り検出符号化されていたか否かが判定される。これは、前段の符号入力部１３１において解析されたヘッダなどに含まれる第２の誤り検出符号化情報を用いて判定可能である。第２の誤り検出符号化情報が“０”の場合（誤り検出符号化されていないと判定された場合）には、処理はステップＳ１４３に進み、暗号解除鍵情報が存在するか否かを判定する。暗号化鍵情報がないと判断した場合には、本処理を終え、下位の処理にそのまま符号化データを出力する。また、暗号化鍵情報が存在すると判断した場合には、ステップＳ１４５で暗号化を解除する処理（暗号復号化処理）を行った後、下位に出力する。

【００５８】

一方、ステップＳ１４１において入力されたビットストリームが、暗号化前に誤り検出符号化されていたと判断した場合、処理はステップＳ１４２に進み、暗号化鍵情報が存在するか否かを判断する。暗号化鍵情報が存在しない場合には本処理を終える。つまり、ステップＳ１４３でのＮｏと判断された場合と同様になる。

【００５９】

また、暗号化鍵情報が存在すると判断した場合、処理をステップＳ１４４に進め、第１の誤り検出符号化情報を“０”から“１”に変更する。即ち、「誤り検出符号化されている」ような情報に変更する。これは、第１の誤り検出符号化情報を“１”とすることにより、圧縮復号処理部において、再び誤り検出機能を動作させるための処理である。

【００６０】

そして、ステップＳ１４５では、入力されたビットストリームに暗号解除鍵情報に基づいて暗号復号処理が施される。暗号復号処理は前述したステップＳ１２４における暗号化処理に対応したものでなければならない。

【００６１】

以上説明したような処理により生成されたヘッダ情報や暗号化されたビットストリームは後段の符号出力部１３３に出力される。

【００６２】

尚、本実施形態においては、第１の誤り検出符号化情報を変更した後に、暗号復号処理を実行するようにしたが、本発明はこれに限定されることなく、図１５に示すように暗号復号処理を実行した後に、第１の誤り検出符号化情報を変更するようにしても良い。

【００６３】

特に、前述した暗号符号化処理部において、第２の誤り検出符号化情報を暗号文の中に含めるようにした場合には、図１５に示すようなフローに従って暗号復号処理を実行する必要がある。これは、第２の誤り検出符号化情報が暗号文の中に含まれている為に、暗号化されている状態では、正しく第２の誤り検出符号化情報を調べることが困難だからである。

【００６４】

そして、符号出力部１３３には、前段の暗号復号処理部１３２で生成されたヘッダ情報や暗号復号されたビットストリームが入力され、暗号復号された符号列として出力される。尚、復号出力部は、更に、前述した圧縮復号出力部に接続され、引き続き圧縮復号処理が実行されるようにしてもよい。

【００６５】

以上説明したように本実施形態によれば、暗号符号化処理を行うことによって、暗号符号化処理された符号列が、誤りが生じていると誤判定されないようにすることが可能となる。

【００６６】

より分かりやすく説明するのであれば、暗号化する装置側で、誤り検出符号を付加したとしても、暗号化処理を行う場合には、見かけ上誤り検出符号データが存在しないことになる（実際には誤り検出符号データは存在するが無視されるだけ）。従って、正しく伝送されている限りは、復号化する装置側では、データに誤りがあると誤判定し、再送の要求を行うことはなくなる。

【００６７】

また、復号化する装置側が暗号化鍵を解除する解除鍵情報を取得している場合には、暗号化が解除（復号）され、誤り検出の符号を利用できるようになるので、万が一、データ伝送中にノイズが入ったとしても、再送を要求し、正常な画像

を再現できるようになる。以上、本実施形態における暗号復号処理部における動作について説明した。

【００６８】

上記本実施形態における暗号復号処理部は、一般に、パーソナルコンピュータ等の情報処理装置で実現できることは容易に類推できよう。また、パーソナルコンピュータ等の情報処理装置で、上記機能を実現すれば良いわけであるから、実施形態での特徴は情報処理方法、更には、コンピュータプログラムや、コンピュータプログラムを格納するＣＤＲＯＭ等のコンピュータ可読記憶媒体にまで及ぶものである。

【００６９】

[第２の実施形態]

上記実施形態（第１の実施形態）では、暗号化前に誤り検出符号化されていたか否かを示す第２の誤り検出符号化情報を必要としたが、本発明はこれに限定されることなく、第２の誤り検出符号化情報を必要としないようにすることも可能である。そこで本第２の実施形態では、第２の誤り検出符号化情報を必要としない方法について説明する。

【００７０】

＜暗号符号化処理部＞

まず、図１６を用いて本実施の形態における暗号符号化処理部について説明する。

【００７１】

図１６において、１６１は符号入力部、１６２はエントロピ復号部、１６３は暗号化処理部、１６４はエントロピ符号化部、１６５は符号出力部である。

【００７２】

符号入力部１６１、エントロピ復号部１６２、エントロピ符号化部１６４、及び符号出力部１６５で実行される各々の処理は、第１の実施形態における符号入力部５１、エントロピ復号部５２、エントロピ符号化部１４、及び符号出力部１５で実行される処理と夫々等しいため、詳細な説明は省略する。そこで、本第２の実施形態では処理が異なる暗号化処理部１６３における暗号化処理についての

詳細を説明する。

【００７３】

図１７は本実施形態に適応可能な暗号化処理を示すフローチャートである。

【００７４】

まず、ステップＳ１７１においてエントロピ復号部１６２を用いてビットプレーン毎に前述したエントロピ復号処理が実行される。続いてステップＳ１７２においてエントロピ復号されたデータに対して暗号化処理が実行される。

【００７５】

次に、ステップＳ１７３で、入力されたビットストリームが誤り検出符号化されているか否かが判定される。これは、前段の符号入力部１６１において解析された符号化パラメータに含まれる第１の誤り検出符号化情報を用いて判定可能である。第１の誤り検出符号化情報が“１”の場合（誤り検出符号化されていると判定された場合）には処理をステップＳ１７４に進み、第１の誤り検出符号化情報が“０”の場合（誤り検出符号化されていないと判定された場合）には処理をステップＳ１７５に進める。

【００７６】

ステップＳ１７４では、前段のステップＳ１７２において暗号化処理が施されたデータの後ろにセグメンテーションシンボルを添付する。これにより、暗号化されたデータに対して誤り検出機能を持たせることが可能である。

【００７７】

ステップＳ１７５では、暗号化されたデータに対してエントロピ符号化部１６４を用いてビットプレーン毎にエントロピ符号化処理を施す。前段のステップＳ１７４においてセグメンテーションシンボルが添付されている場合には、セグメンテーションシンボルも含めてエントロピ符号化処理を施すようにする。

【００７８】

以上説明したような処理により生成されたヘッダ情報や暗号化されたビットストリームは後段の符号出力部１６５に出力される。

【００７９】

＜暗号復号処理部＞

次に、実施形態における画像データを復号化（再生する）側の処理について説明する。

【００８０】

図１８は本第２の実施形態に適応可能な暗号復号処理部のブロック構成図である。同図において、１８１は符号入力部、１８２はエントロピ復号部、１８３は暗号復号部、１８４はエントロピ符号化部、１８５は符号出力部である。図５における符号入力部５１は、符号化部１８５から出力されるデータを入力すると考えると分かりやすい。

【００８１】

第１の実施形態（図１３）と処理が異なるのは、暗号復号処理部１６３と、その前後にエントロピー復号部１６３、エントロピー符号化部１６４を設けた点である。エントロピー復号部１６３、同符号化部１６４については、暗号化装置での処理と同じであるので、ここでは、暗号復号部１８３における暗号復号処理についての詳細を図１９を用いて説明する。

【００８２】

まず、ステップＳ１９１において、暗号化解除鍵情報が存在するか否かを判断する。否の場合には、本処理を終える。

【００８３】

また、暗号化解除鍵情報が存在する場合、処理はステップＳ１９２に進み、エントロピ復号部１８２を用いてビットプレーン毎に前述したエントロピ復号処理が実行される。続いてステップＳ１９３においてエントロピ復号されたデータに対して暗号復号処理が実行される。そして、ステップＳ１９３で実行される暗号復号処理は、前述したステップＳ１７２に対応する処理でなければならない。そしてステップＳ１９４においてエントロピ符号化部１８４を用いてビットプレーン毎に前述したエントロピ符号化処理が実行される。

【００８４】

以上説明したような処理により生成されたヘッダ情報や暗号復号されたビットストリームは後段の符号出力部１８５に出力され、図５で示される処理に渡されることになる。

【００８５】

以上説明したように暗号符号化処理を行うことによって、暗号化されたデータに対しても誤り検出符号化機能を有するようにすることが可能となる。

【００８６】

以上、本実施形態における暗号符号化処理部、及び暗号復号処理部における動作について説明した。上記本実施形態における暗号符号化処理部、暗号復号処理部は、一般に、パーソナルコンピュータ等の情報処理装置で実現できることは容易に類推できよう。また、パーソナルコンピュータ等の情報処理装置で、上記機能を実現すれば良いわけであるから、実施形態での特徴は情報処理方法、更には、コンピュータプログラムや、コンピュータプログラムを格納するＣＤＲＯＭ等のコンピュータ可読記憶媒体にまで及ぶものである。

【００８７】

［第３の実施形態］

上記第２の実施形態においては、ＪＰＥＧ２０００などを想定して誤り検出符号化処理が、エントロピ符号化（図１におけるエントロピー符号化部１４）内で実行される例を説明した。しかしながら本発明はこれに限定されることない。すなわち、暗号化した際の、誤り検出符号の付加を単独で実行するようにしても良い。以下、この例を第３の実施形態として説明する。

【００８８】

＜暗号符号化処理部＞

まず、図２０を用いて本実施の形態における暗号符号化処理部（暗号符号化装置）について説明する。

【００８９】

図２０において、２０１は符号入力部、２０２は暗号符号化部、２０３は誤り検出符号化部、２０４は符号出力部である。符号化部２０１は、図１における符号化部１５の出力結果を入力するものとすると分かりやすいが、符号入力部２０１が入力する符号化ストリームはこれに限らず、他の圧縮符号化処理で生成されたものでも良い。

【００９０】

図２１は本実施形態に適応可能な暗号化処理、及び誤り訂正符号化処理を示すフローチャートである。

【００９１】

まず、ステップＳ２１１で、暗号化処理部２０２を用いて、入力されたビットストリームに対して暗号化処理が実行される。注意したいのは、入力したビットストリームは、画像データそのものの符号化データに、誤り検出符号が付加されていてる場合と、それが付加されていない場合がある点である。また、ここで言う暗号化処理は、入力した符号化データが「画像データの符号化データ＋誤り検出符号データ」である場合には、その誤り検出を含めて暗号化する。誤り検出符号が存在しない場合には、当然暗号化対象は「画像データの符号化データ」のみとなる。従って、入力した符号化データが「画像データの符号化データ＋誤り検出符号データ」である場合には、暗号化後にはその区別がない１つのストリームが生成されることになる。

【００９２】

次いで、ステップＳ２１２に進み、暗号化処理を行った符号化データに誤り検出符号データが存在したか否かを判断する。この判断は、第１、第２の実施形態で述べた、第１の誤り検出符号化情報を参照する等で対処できるであろうし、場合によっては現実に誤り検出符号データを検出できたか否かで判断してもよい。

【００９３】

いずれにせよ、「誤り検出符号データ」というのは、画像符号化データの信頼性を高めたいという現れである。従って、ステップＳ２１２での判断でＹＥＳになった場合には、暗号化したデータの伝送の信頼性を高くするため、ステップＳ２１３で誤り検出符号化をおこなう。また、ステップＳ２１２でＮｏになった場合には、もともと誤り検出符号が行われていないわけであるから、ステップＳ２１３の処理はおこなわない。

【００９４】

以上説明したように暗号符号化処理を行うことによって、暗号化されたデータに対しても誤り訂正符号化機能を有するようにすることが可能となる。

【００９５】

以上、本実施形態における暗号符号化処理部、及び暗号復号処理部における動作について説明した。上記本実施形態における暗号符号化処理部、暗号復号処理部は、一般に、パーソナルコンピュータ等の情報処理装置で実現できることは容易に類推できよう。また、パーソナルコンピュータ等の情報処理装置で、上記機能を実現すれば良いわけであるから、実施形態での特徴は情報処理方法、更には、コンピュータプログラムや、コンピュータプログラムを格納するＣＤＲＯＭ等のコンピュータ可読記憶媒体にまで及ぶものである。

【００９６】

以上本発明にかかる実施形態を説明したが、上記実施形態に係る実施態様を列挙すると、次の通りである。

【００９７】

[実施態様１]　符号化画像データを暗号化する情報処理方法であって、

符号化画像データを入力する工程と、

入力した符号化画像データを暗号化する工程と、

符号化データのヘッダ部中の誤り検出符号有無を示す有無情報を、誤り検出符号無しに変更し、暗号化した符号化画像データを出力する工程と

を備えることを特徴とする情報処理方法。

【００９８】

[実施態様２]　更に、暗号化を解除する暗号化解除鍵情報を出力する工程を備えることを特徴とする実施態様１に記載の情報処理方法。

【００９９】

[実施態様３]　更に、入力した符号化画像データ中の前記有無情報を、前記ヘッダ部内の他の位置に待避する工程を備えることを特徴とする実施態様１に記載の情報処理方法。

【０１００】

[実施態様４]　前記待避する工程では、前記ヘッダ部にコメントとして待避することを特徴とする実施態様２に記載の情報処理方法。

【０１０１】

[実施態様５]　実施態様３に記載の情報処理方法で暗号化された画像デー

タを復号する情報処理方法であって、

符号化画像データを入力する工程と、

前記待避した前記有無情報が、誤り検出有りを示すか否かを判定する第１の判定工程と、

暗号化を解除する鍵情報があるか否かを判定する第２の判定工程と、

前記第１、第２の判定工程によって、誤り検出符号有り、及び、暗号化解除鍵情報有りと判定した場合、前記ヘッダ部内の有無情報を誤り検出有りに変更すると共に、暗号化を解除し、符号化画像データの復号処理に渡す工程と

を備えることを特徴とする情報処理方法。

【０１０２】

[実施態様６]　前記第１、第２の判定工程によって、誤り検出符号無し、及び、暗号化解除鍵情報有りと判定した場合には、前記ヘッダ部内の有無情報を変更せず、暗号化を解除することを特徴とする実施態様５に記載の情報処理方法。

【０１０３】

[実施態様７]　前記第１、第２の判定工程によって、暗号化解除鍵情報無しと判定した場合には、入力した符号化画像データをそのまま符号化画像データの復号処理に渡すことを特徴とする実施態様５に記載の情報処理方法。

【０１０４】

[実施態様８]　符号化画像データを暗号化する情報処理装置であって、

符号化画像データを入力する手段と、

入力した符号化画像データを暗号化する手段と、

符号化データのヘッダ部中の誤り検出符号有無を示す有無情報を、誤り検出符号無しに変更し、暗号化した符号化画像データを出力する手段と

を備えることを特徴とする情報処理装置。

【０１０５】

[実施態様９]　更に、入力した符号化画像データ中の前記有無情報を、前記ヘッダ部内の他の位置に待避する手段を備えることを特徴とする実施態様８に記載の情報処理装置。

【０１０６】

[実施態様１０]　実施態様９に記載の情報処理装置で暗号化された画像データを復号する情報処理装置であって、

符号化画像データを入力する手段と、

前記待避した前記有無情報が、誤り検出有りを示すか否かを判定する第１の判定手段と、

暗号化を解除する鍵情報があるか否かを判定する第２の判定手段と、

前記第１、第２の判定工程によって、誤り検出符号有り、及び、暗号化解除鍵情報有りと判定した場合、前記ヘッダ部内の有無情報を誤り検出有りに変更すると共に、暗号化を解除し、符号化画像データの復号処理に渡す手段と

を備えることを特徴とする情報処理装置。

【０１０７】

[実施態様１１]　コンピュータが読み込み実行することで、符号化画像データを暗号化する情報処理装置として機能するコンピュータプログラムであって、

符号化画像データを入力する手段と、

入力した符号化画像データを暗号化する手段と、

符号化データのヘッダ部中の誤り検出符号有無を示す有無情報を、誤り検出符号無しに変更し、暗号化した符号化画像データを出力する手段と

して機能することを特徴とするコンピュータプログラム。

【０１０８】

[実施態様１２]　更に、入力した符号化画像データ中の前記有無情報を、前記ヘッダ部内の他の位置に待避する手段として機能することを特徴とする実施態様１１に記載のコンピュータプログラム。

【０１０９】

[実施態様１３]　実施態様１１又は１２に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

【０１１０】

[実施態様１４]　コンピュータが読み込み実行することで、実施態様９に

記載の情報処理装置で暗号化された画像データを復号する情報処理装置として機能するコンピュータプログラムであって、

符号化画像データを入力する手段と、

前記待避した前記有無情報が、誤り検出有りを示すか否かを判定する第１の判定手段と、

暗号化を解除する鍵情報があるか否かを判定する第２の判定手段と、

前記第１、第２の判定工程によって、誤り検出符号有り、及び、暗号化解除鍵情報有りと判定した場合、前記ヘッダ部内の有無情報を誤り検出有りに変更すると共に、暗号化を解除し、符号化画像データの復号処理に渡す手段と

して機能することを特徴とするコンピュータプログラム。

【０１１１】

［実施態様１５］　実施態様１４に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

【０１１２】

［実施態様１６］　符号化画像データを暗号化する情報処理方法であって、

符号化画像データを入力する工程と、

入力した圧縮符号化画像データを復号し、暗号化する工程と、

入力した圧縮符号化画像データのヘッダ部中の誤り検出符号の有無を示す有無情報を判定する工程と、

該判定工程で誤り検出符号無しと判定した場合には暗号化した画像データを再符号化し、誤り検出符号有りと判定した場合、前記暗号化工程で暗号化した画像データに誤り検出符号有りを示すセグメンテーションシンボルを付加して再符号化する再符号化制御工程と

を備えることを特徴とする情報処理方法。

【０１１３】

［実施態様１７］　前記復号工程はエントロピー復号、前記再符号化制御工程ではエントロピー符号を行うことを特徴とする実施態様１６に記載の情報処理方法。

【０１１４】

［実施態様１８］　実施態様１６又は実施態様１７に記載の情報処理方法で暗号化、符号化された画像データを復号するための情報処理方法であって、

暗号化され、符号化画像データを入力する工程と、

暗号化状態に復元するため、前記入力工程で入力した符号化画像データを復号する工程と、

暗号化を解除する鍵情報に基づいて暗号化を解除し、再符号化を行う符号化工程と、

再符号化した符号化データを、下位に位置する圧縮符号化画像データの復号処理に出力する工程とを備えることを特徴とする情報処理方法。

【０１１５】

［実施態様１９］　符号化画像データを暗号化する情報処理装置であって、

符号化画像データを入力する手段と、

入力した圧縮符号化画像データを復号し、暗号化する手段と、

入力した圧縮符号化画像データのヘッダ部中の誤り検出符号の有無を示す有無情報を判定する手段と、

該判定手段で誤り検出符号無しと判定した場合には暗号化した画像データを再符号化し、誤り検出符号有りと判定した場合、前記暗号化手段で暗号化した画像データに誤り検出符号有りを示すセグメンテーションシンボルを付加して再符号化する再符号化制御手段と

を備えることを特徴とする情報処理装置。

【０１１６】

［実施態様２０］　前記復号手段はエントロピー復号、前記再符号化制御手段ではエントロピー符号を行うことを特徴とする実施態様１９に記載の情報処理装置。

【０１１７】

［実施態様２１］　実施態様１９又は実施態様２０に記載の情報処理装置で暗号化、符号化された画像データを復号するための情報処理装置であって、

暗号化され、符号化画像データを入力する手段と、

暗号化状態に復元するため、前記入力工程で入力した符号化画像データを復号

する手段と、

暗号化を解除する鍵情報に基づいて暗号化を解除し、再符号化を行う符号化手段と、

再符号化した符号化データを、下位に位置する圧縮符号化画像データの復号処理に出力する手段と

を備えることを特徴とする情報処理装置。

【０１１８】

[実施態様２２]　コンピュータが読み込み実行することで、符号化画像データを暗号化する情報処理装置として機能するコンピュータプログラムであって、

符号化画像データを入力する手段と、

入力した圧縮符号化画像データを復号し、暗号化する手段と、

入力した圧縮符号化画像データのヘッダ部中の誤り検出符号の有無を示す有無情報を判定する手段と、

該判定手段で誤り検出符号無しと判定した場合には暗号化した画像データを再符号化し、誤り検出符号有りと判定した場合、前記暗号化手段で暗号化した画像データに誤り検出符号有りを示すセグメンテーションシンボルを付加して再符号化する再符号化制御手段と

して機能することを特徴とするコンピュータプログラム。

【０１１９】

[実施態様２３]　前記復号手段はエントロピー復号、前記再符号化制御手段ではエントロピー符号を行うことを特徴とする実施態様２２に記載のコンピュータプログラム。

【０１２０】

[実施態様２４]　実施態様２２又は実施態様２３に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

【０１２１】

[実施態様２５]　コンピュータが読み込み実行することで、実施態様１９又は実施態様２０に記載の情報処理装置で暗号化、符号化された画像データを復

号するための情報処理装置として機能するコンピュータプログラムであって、

暗号化され、符号化画像データを入力する手段と、

暗号化状態に復元するため、前記入力工程で入力した符号化画像データを復号する手段と、

暗号化を解除する鍵情報に基づいて暗号化を解除し、再符号化を行う符号化手段と、

再符号化した符号化データを、下位に位置する圧縮符号化画像データの復号処理に出力する手段と

して機能することを特徴とするコンピュータプログラム。

【０１２２】

[実施態様２６]　実施態様２５に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

【０１２３】

【発明の効果】

以上説明したように本発明によれば、誤り検出符号が付加された圧縮符号化画像データを暗号化したとしても、それを受信し再生する側の装置において無意味な再送要求等を行わず、正常な処理を行えるようになる。

【図面の簡単な説明】

【図１】

実施形態における圧縮符号化処理部の構成を示す図である。

【図２】

実施形態における離散ウェーブレット変換部を説明する図である。

【図３】

実施形態におけるエントロピ符号化の説明をする図である。

【図４】

実施形態における符号列の説明をする図である。

【図５】

実施形態における圧縮復号処理部の構成を示す図である。

【図６】

実施形態におけるエントロピ復号の説明をする図である。

【図７】

実施形態における逆離散ウェーブレット変換部を説明する図である。

【図８】

実施形態における階層的な圧縮復号を説明する図である。

【図９】

実施形態におけるシステム全体の構成図である。

【図１０】

実施形態における誤り検出符号付きのデータの構造を示す図である。

【図１１】

第１の実施形態における暗号符号化処理部の構成を示す図である。

【図１２】

第１の実施形態における暗号化処理手順を示すフローチャートである。

【図１３】

第１の実施形態における暗号復号処理部の構成を示す図である。

【図１４】

第１の実施形態における暗号復号処理手順を示すフローチャートである。

【図１５】

第１の実施形態における暗号復号処理の他のフローチャートである。

【図１６】

第２の実施形態における暗号符号化処理部の構成を示す図である。

【図１７】

第２の実施形態における暗号化処理手順を示すフローチャートである。

【図１８】

第２の実施形態における暗号復号処理部の構成を示す図である。

【図１９】

第２の実施形態における暗号復号処理手順を示すフローチャートである。

【図２０】

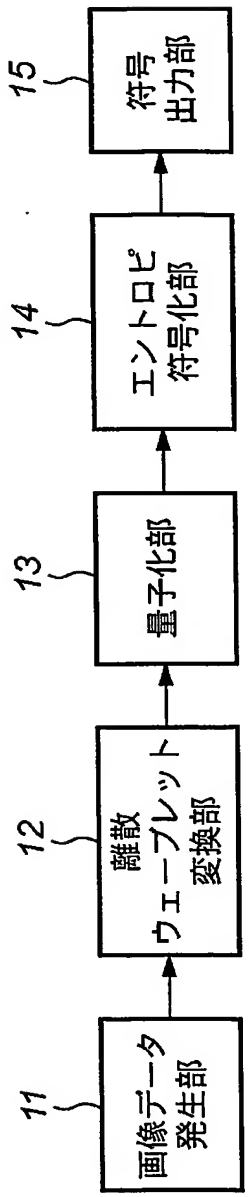
第３の実施形態における暗号符号化処理の構成を説明する図である。

【図２１】

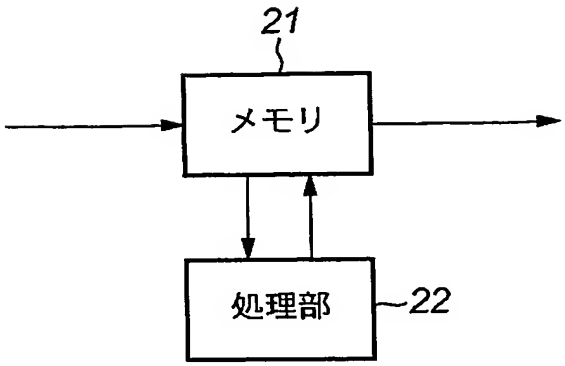
第３の実施形態における暗号符号化処理、及び誤り訂正符号化処理手順を示すフローチャートである。

【書類名】　図面

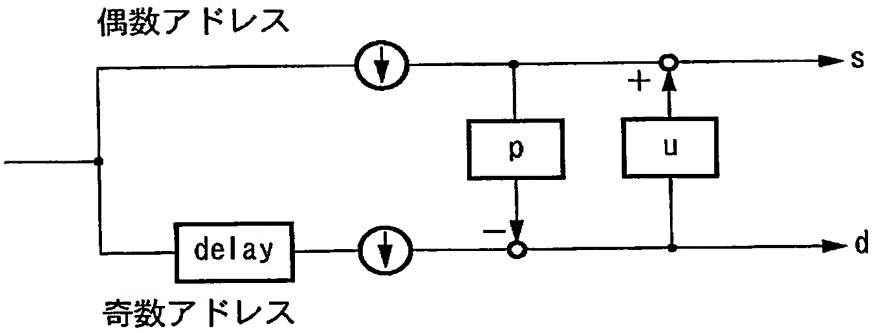
【図１】



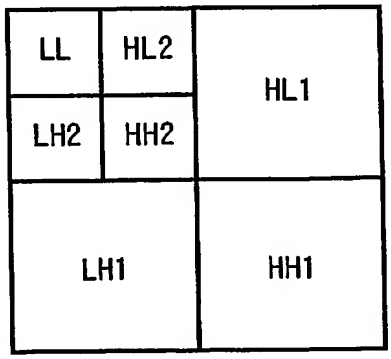
【図２】


21
メモリ
処理部
22

(a)

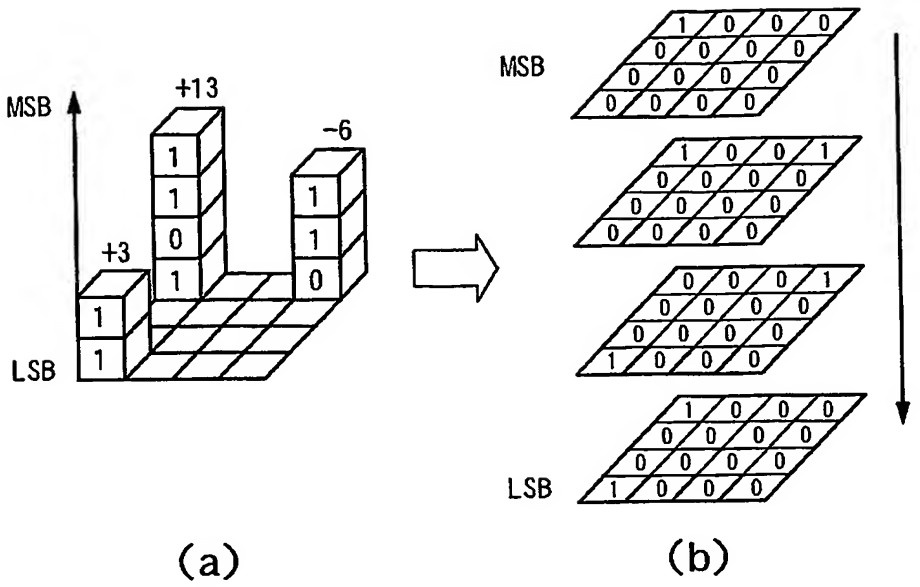

偶数アドレス
s
+
p
u
delay
−
d
奇数アドレス

(b)

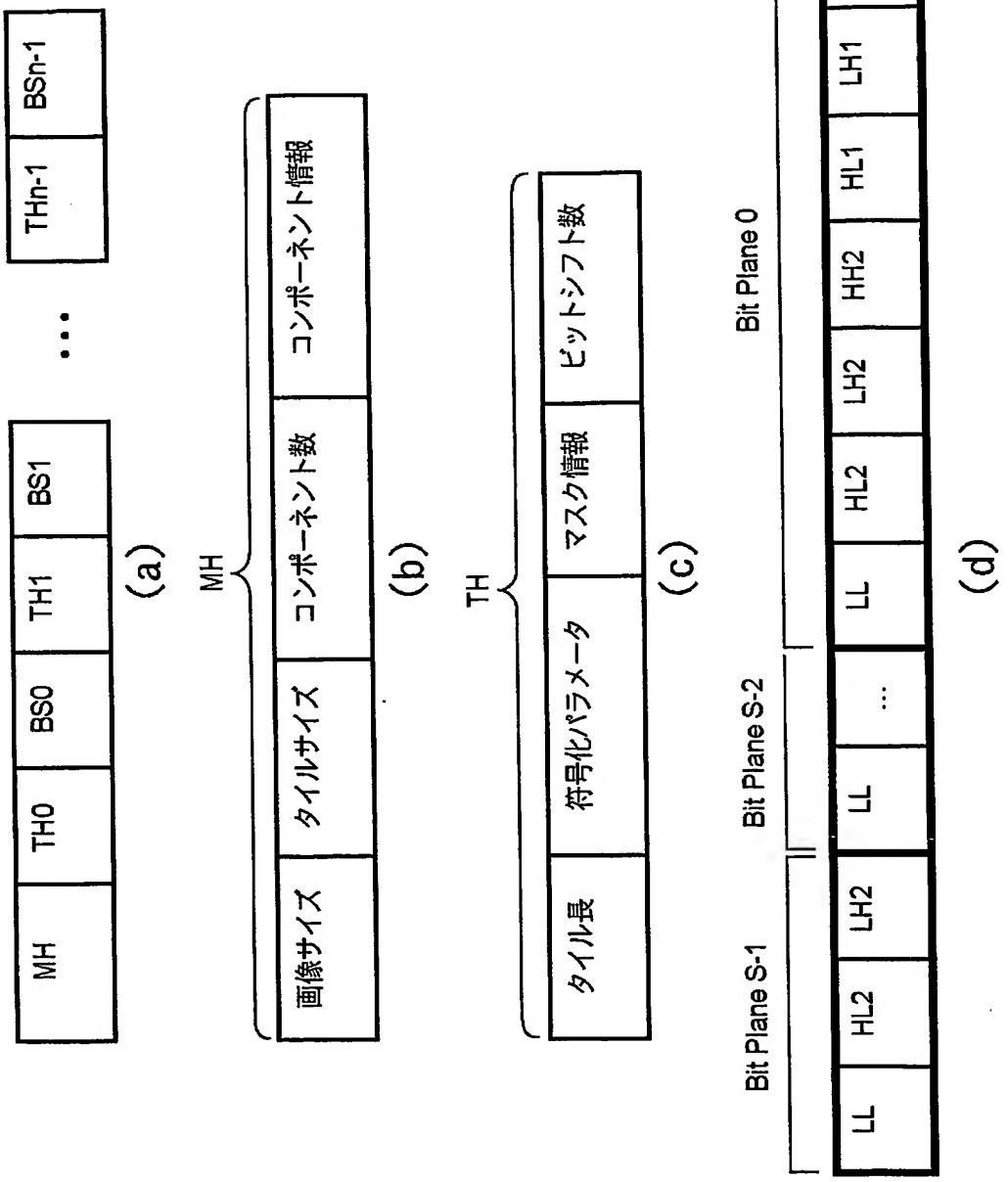

LL
HL2
HL1
LH2
HH2
LH1
HH1

(c)

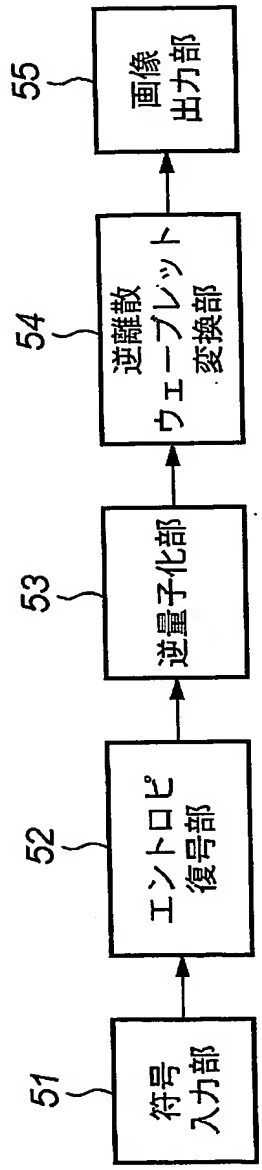
【図３】



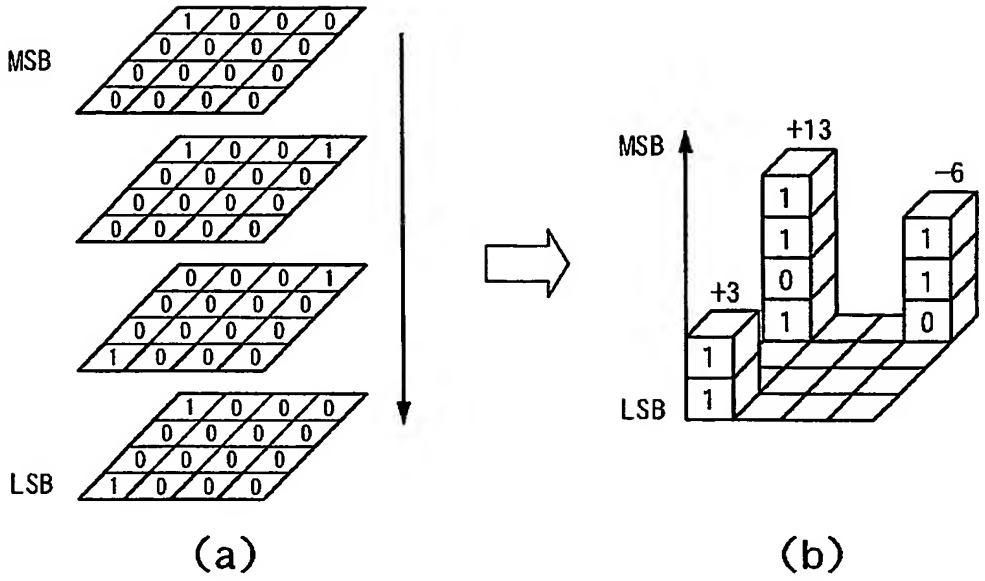
【図４】


MH
TH0
BS0
TH1
BS1
THn-1
BSn-1
(a)
MH
画像サイズ
タイルサイズ
コンポーネント数
コンポーネント情報
(b)
TH
タイル長
符号化パラメータ
マスク情報
ビットシフト数
(c)
Bit Plane 0
Bit Plane S-2
Bit Plane S-1
LL
HL2
LH2
LL
...
LL
HL2
LH2
HH2
HL1
LH1
HH1
(d)

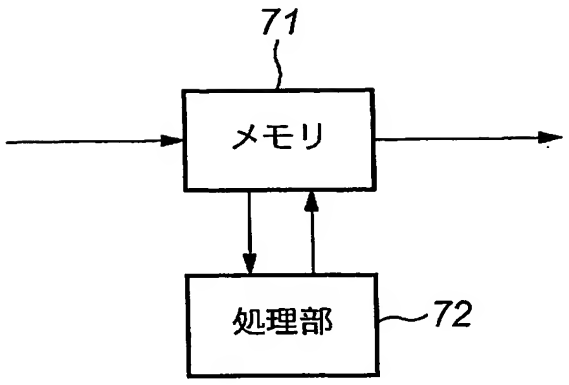
【図５】



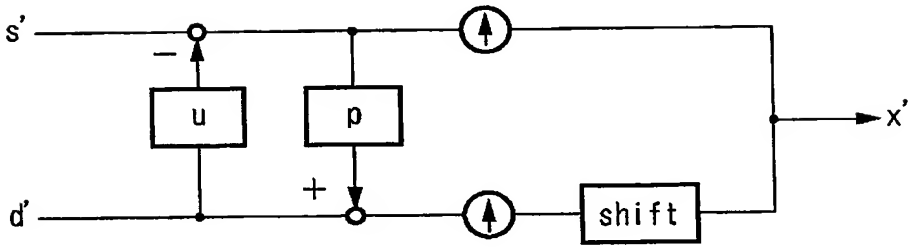
【図６】



【図７】

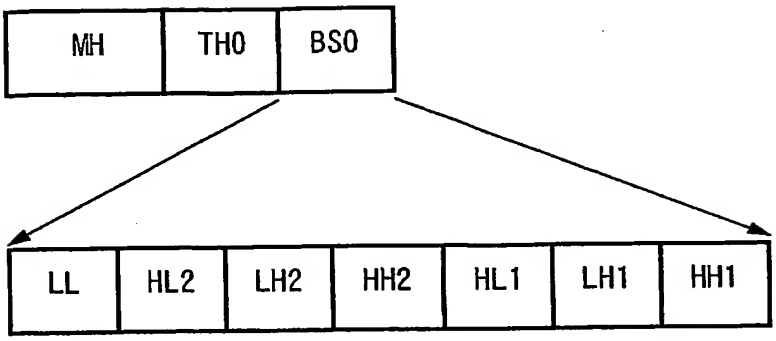


(a)



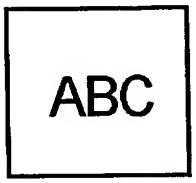
(b)

【図８】

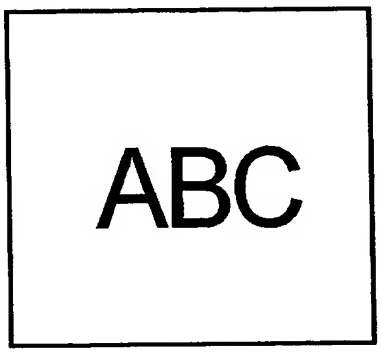


(a)

=LL



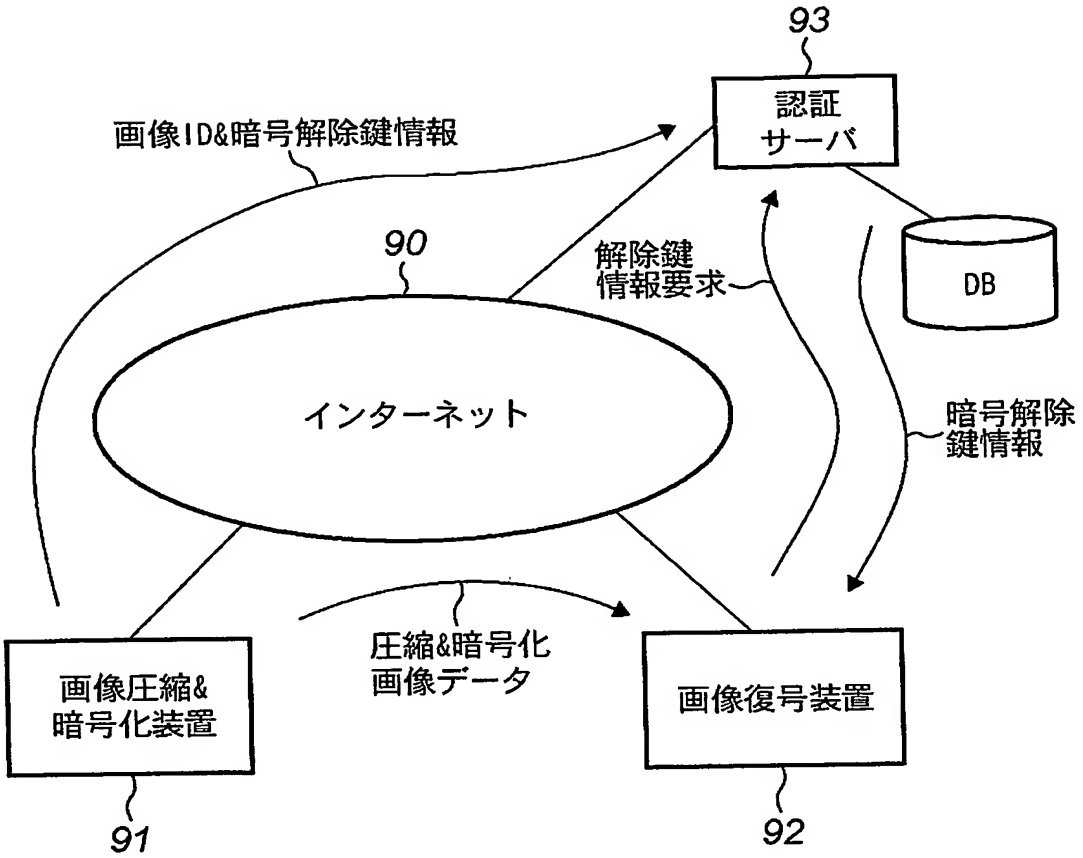
=LL+HL2+LH2+HH2



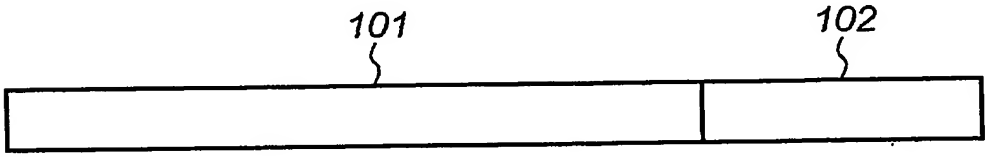
=LL+HL2+LH2+HH2+HL1+LH1+HH1

(b)

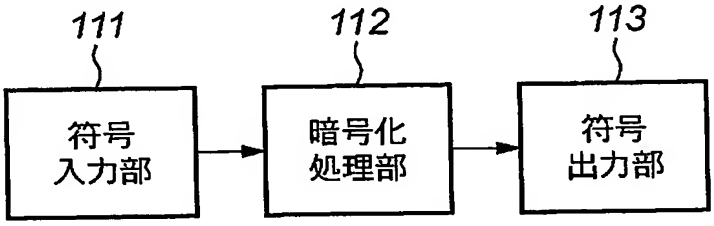
【図９】


93
認証
サーバ
画像ID&暗号解除鍵情報
90
解除鍵
情報要求
DB
インターネット
暗号解除
鍵情報
圧縮&暗号化
画像データ
画像圧縮&
暗号化装置
画像復号装置
91
92

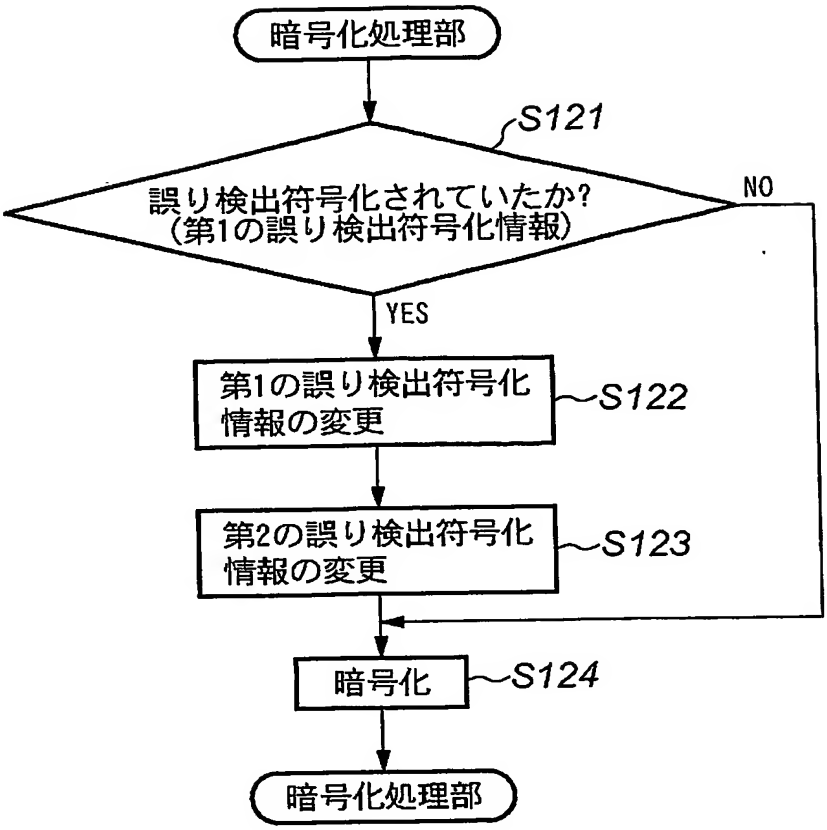
【図１０】


101
102

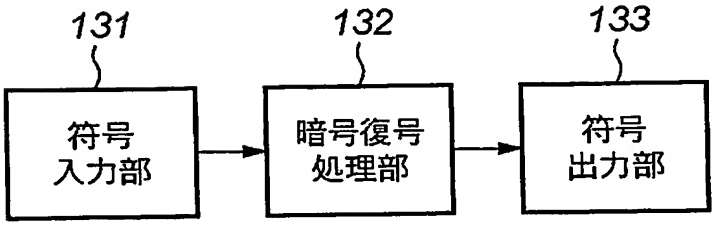
【図１１】


111
112
113
符号
入力部
暗号化
処理部
符号
出力部

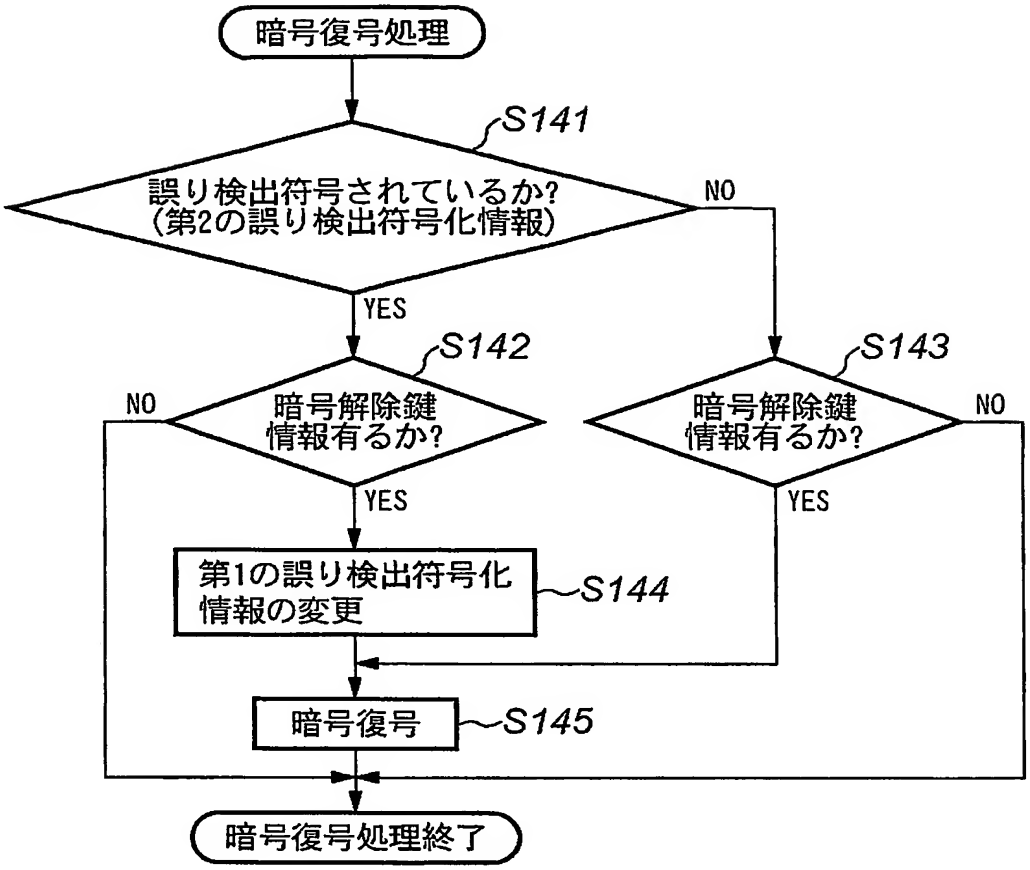
【図１２】


暗号化処理部
S121
誤り検出符号化されていたか?
(第1の誤り検出符号化情報)
NO
YES
第1の誤り検出符号化
情報の変更
S122
第2の誤り検出符号化
情報の変更
S123
暗号化
S124
暗号化処理部

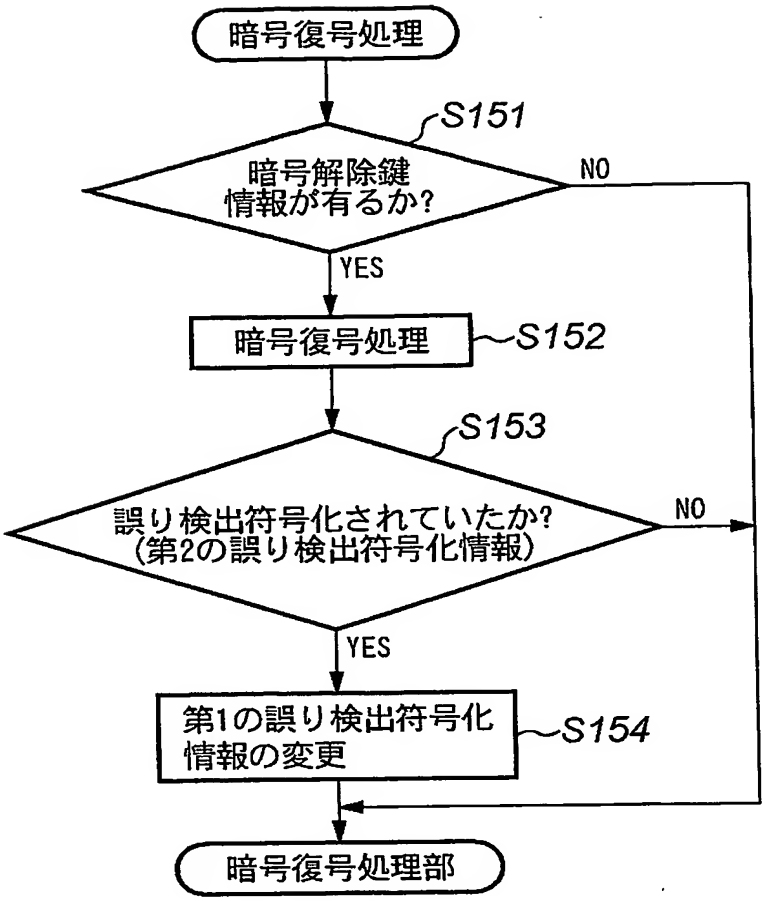
【図１３】


131
132
133
符号
入力部
暗号復号
処理部
符号
出力部

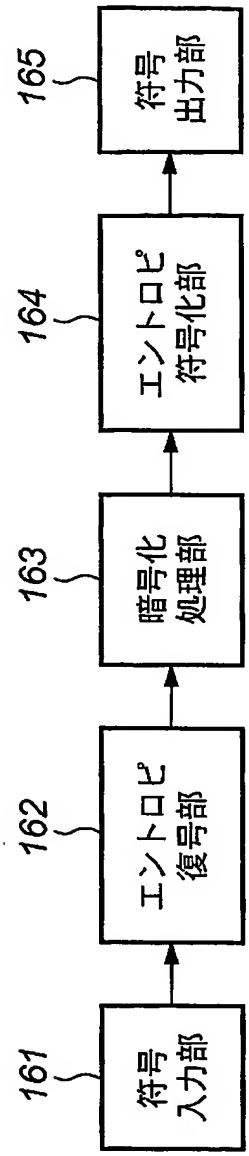
【図１４】


暗号復号処理
S141
誤り検出符号されているか?
(第2の誤り検出符号化情報)
NO
YES
S142
暗号解除鍵
情報有るか?
NO
YES
S143
暗号解除鍵
情報有るか?
NO
YES
第1の誤り検出符号化
情報の変更
S144
暗号復号
S145
暗号復号処理終了

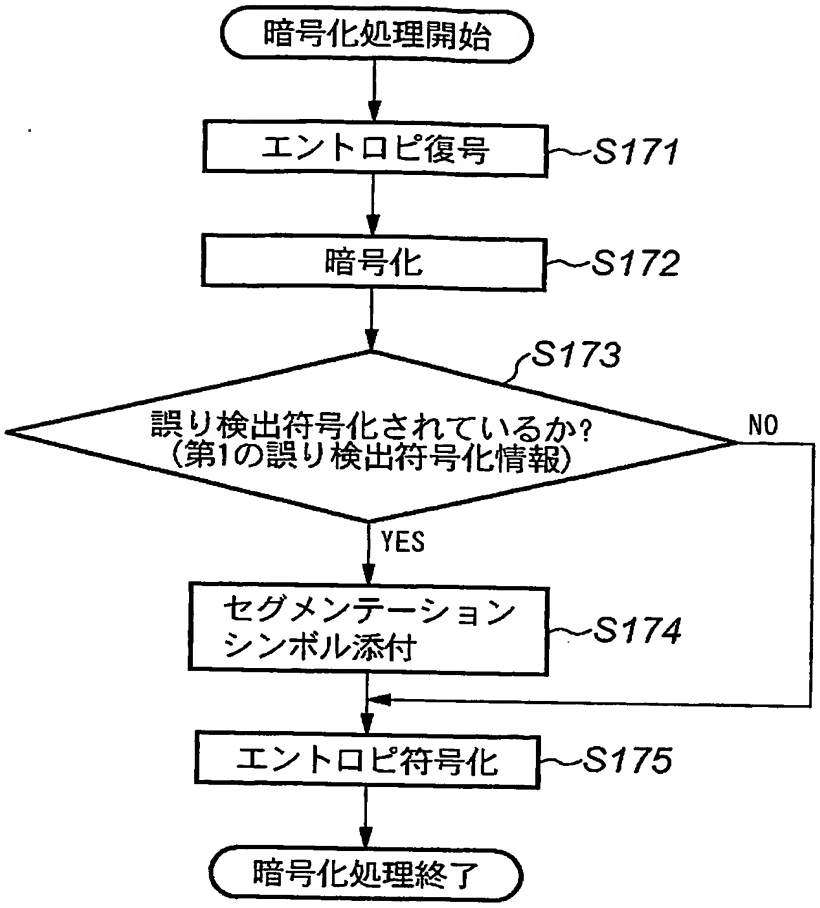
【図１５】


暗号復号処理
S151
暗号解除鍵
情報が有るか?
NO
YES
暗号復号処理
S152
S153
誤り検出符号化されていたか?
(第2の誤り検出符号化情報)
NO
YES
第1の誤り検出符号化
情報の変更
S154
暗号復号処理部

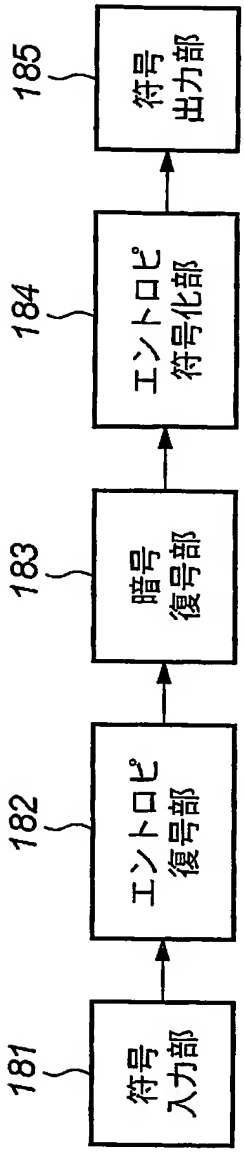
【図１６】



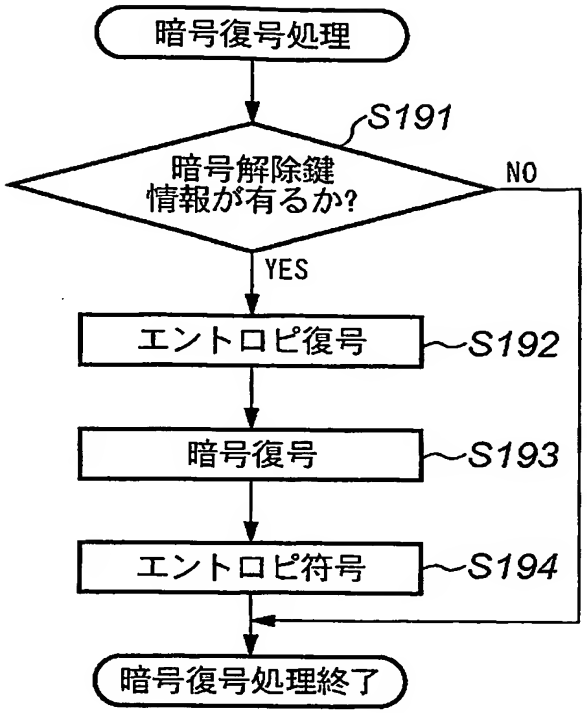
【図１７】


暗号化処理開始
エントロピ復号
S171
暗号化
S172
S173
誤り検出符号化されているか?
(第1の誤り検出符号化情報)
NO
YES
セグメンテーション
シンボル添付
S174
エントロピ符号化
S175
暗号化処理終了

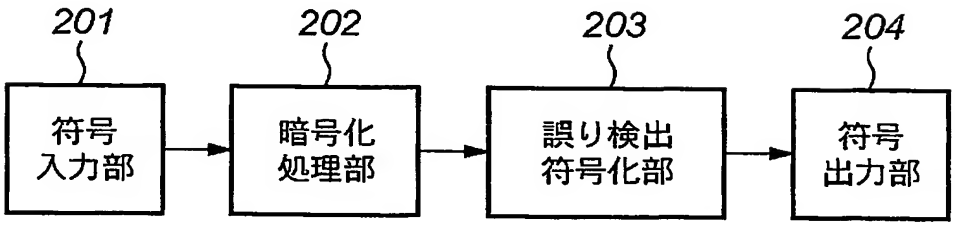
【図１８】



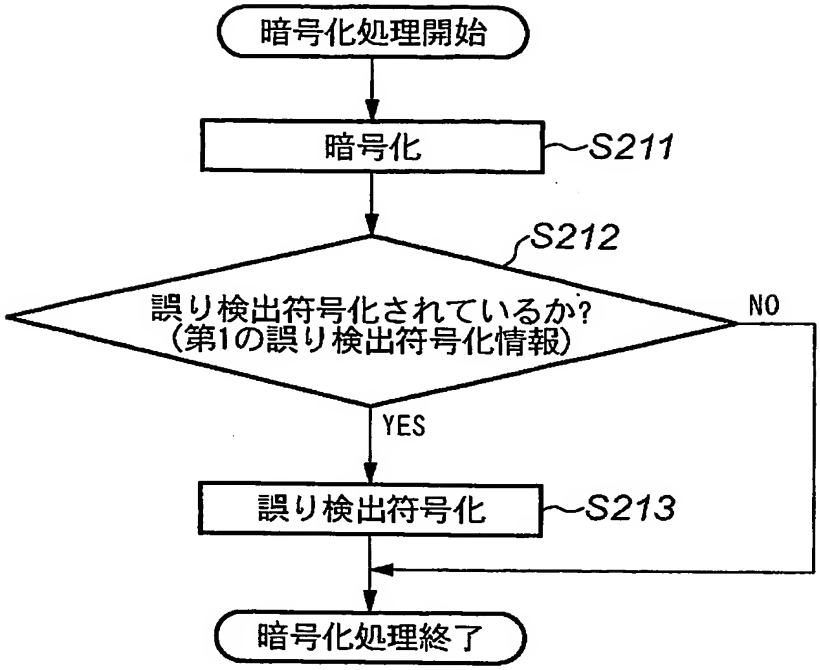
【図１９】


暗号復号処理
S191
暗号解除鍵
情報が有るか?
NO
YES
エントロピ復号
S192
暗号復号
S193
エントロピ符号
S194
暗号復号処理終了

【図２０】


201
202
203
204
符号
入力部
暗号化
処理部
誤り検出
符号化部
符号
出力部

【図２１】


暗号化処理開始
暗号化
S211
S212
誤り検出符号化されているか?
(第1の誤り検出符号化情報)
NO
YES
誤り検出符号化
S213
暗号化処理終了

【書類名】　要約書

【課題】　誤り検出符号が付加された圧縮符号化画像データを暗号化したとしても、それを受信し再生する側の装置において無意味な再送要求等を行わず、正常な処理を行えるようになる。

【解決手段】　圧縮符号化された画像データを入力し、そのヘッダ部にある第１の誤り検出符号情報を調べることで、誤り検出符号が付加されているか否かを判定する（Ｓ１２１）。誤り検出符号が付加されていると判断した場合には、その第１の誤り検出符号情報を誤り検出符号無しに変更し（Ｓ１２２）、第２の誤り検出符号情報として待避する（Ｓ１２３）。そして、符号化画像データを暗号化する（Ｓ１２４）。

【選択図】　図１２

特願２００３－０１５２３３

出願人履歴情報

識別番号 [０００００１００７]

１．変更年月日 １９９０年 ８月３０日
[変更理由] 新規登録
住所 東京都大田区下丸子３丁目３０番２号
氏名 キヤノン株式会社